



Understanding Secure Audio Path



- ⌘ *What are the benefits?*
- ⌘ *How does it work?*
- ⌘ *How does this affect the consumer experience?*
- ⌘ *How do I implement it?*
- ⌘ *Where can I get more information?*

Understanding Secure Audio Path

Online piracy of copyrighted material has exploded on the Internet with thousands of songs being distributed illegally every day. Content owners have been using various technologies like encryption, fingerprinting, and watermarking to curb piracy. Even when content is protected with these technologies, it is possible that consumers can still use third-party programs to capture protected content. These pirate programs allow consumers to create digital copies that they can trade online through file-swapping programs. In order to protect digital content from this form of online piracy, content owners must look beyond current encryption technologies for solutions that provide end-to-end protection of their valuable assets.

Secure Audio Path (SAP) is a feature of Microsoft® Windows® Millennium Edition and Windows XP that enhances Microsoft's DRM technology—the Windows Media™ Rights Manager Software Development Kit (SDK). SAP provides an infrastructure for maintaining copy protection for music by ensuring that it is not intercepted by an unauthorized application before it reaches the sound card on a consumer's computer. Secure Audio Path gives *content owners* an added level of protection against piracy when distributing content online.

What are the benefits?

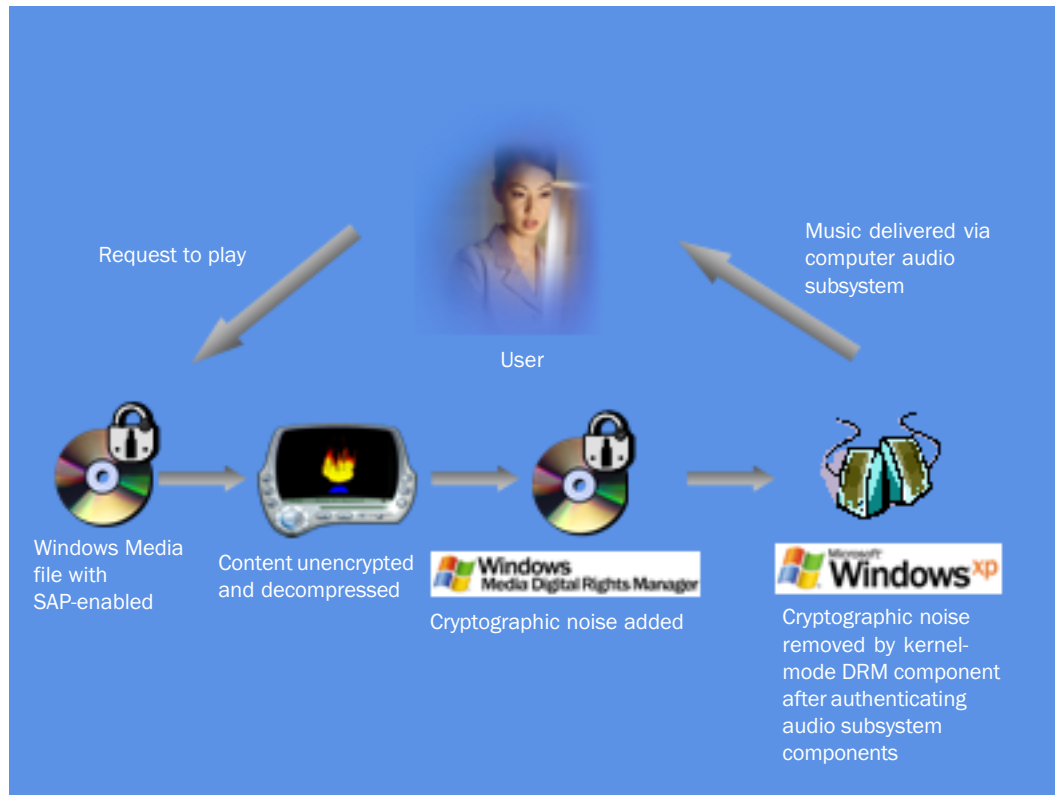
The Secure Audio Path model provides content owners with the following benefits:

- **Deepest level of protection.** Both streamed and downloaded content are ensured protection until they reach the consumer's sound card in both Windows Millennium Edition and Windows XP.
- **Ability to prevent digital copying.** Consumers will not be able to make perfect digital copies of SAP-enabled music after it has been decrypted.
- **Ability to set security levels for sound cards.** Content owners can require that sound cards meet certain security levels before a consumer can download digital music.
- **Not restricted to Windows Media Player.** Any third-party developer can build a player based on the Windows Media Format SDK and take advantage of the improved security of Secure Audio Path.



How does it work?

In the Secure Audio Path model, a consumer attempts to play a Windows Media file that was protected with the Windows Media Rights Manager SDK and has the Secure Audio Path feature enabled. The encrypted content is sent to a player where it is decompressed and decrypted. Then noise is added to the signal and is removed only when the audio components have been authenticated as shown in the following figure.



If pirate applications try to intercept the audio signal before the audio components are authenticated, consumers will hear only random noise.

Along with deterring audio piracy, Secure Audio Path can also work with Windows Media-based video files to help deter video piracy. Pirate applications are able to capture the video part of a file; however, consumers hear only random noise while watching the captured video.

How does this affect the consumer experience?

The effect of Secure Audio Path on most consumers' experience is transparent. It works silently in the background and does not require any action by consumers. They simply select the content they want to play and listen to it. This section describes the consumer experience for three scenarios: acquisition of SAP-enabled content, playing pirated SAP-enabled content, and playing content other than Windows Media-based content.

Acquiring SAP-enabled content

When consumers request a license for SAP-enabled content, license servers can detect if consumers do not have either Windows Millennium Edition or Windows XP before sending them SAP licenses. If consumers do not have either the correct operating system or the correct certified drivers then they will receive a message informing them of the problem. The SAP-enabled content will not play until all of the requirements of the license are met.

Playing pirated SAP-enabled content

When consumers play pirated SAP-enabled content that they acquire from file swapping or stream capturing, they hear only random noise. By using the deep level of protection that SAP provides, it becomes much harder to distribute digital copies of any SAP-enabled content.

Playing content other than Windows Media-based content

Although Secure Audio Path protects Windows Media files, it does not protect any other files, such as .mp3 or files copied from a personal CD. Secure Audio Path works only with Windows Media files that content owners enable with SAP. This means that the consumers' listening experience is not affected if they are not playing Windows Media files.

How do I implement it?

Secure Audio Path can accommodate all of the different business scenarios by having different levels of protection available. With this level of control, content owners can make sure consumers have all of the proper drivers installed, or that their sound card works with all of the advanced settings of Secure Audio Path.

Content owners can choose how to implement Secure Audio Path by enabling different features, as described in the following table.

Secure Audio Path level	SAP required	Device verified	Digital output disabled
Secure Audio Path is not required. Content works on Microsoft Windows 98, Windows NT® version 4.0 (with Service Pack 6), Windows 2000, Windows Millennium Edition, and Windows XP.	No	No	No
This level is the weakest, but permits a larger number of consumers initially. This mode enables you to secure your files with SAP without checking for certified drivers or disabling the digital output capabilities of sound cards. Supported on Windows Millennium Edition and Windows XP.	Yes	No	No
This level ensures that consumers are using SAP-certified drivers, but the digital output capabilities of sound cards are not disabled. Supported on Windows Millennium Edition and Windows XP.	Yes	Yes	No
This level currently offers the highest level of security. Supported on Windows Millennium Edition and Windows XP.	Yes	Yes	Yes

Where can I get more information?

Secure Audio Path, along with Windows Millennium Edition or Windows XP, helps ensure that content owners are providing a rich listening experience to consumers and protecting their intellectual property rights at the same time. To learn more about the benefits of Secure Audio Path or other DRM features, see the Windows Media Rights Manager SDK at the Microsoft Web site (<http://www.microsoft.com/windows/windowsmedia/en/wm7/drm.asp>).

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2001 Microsoft Corporation. All rights reserved.

Microsoft, Windows, the Windows logo, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Microsoft